6. What can you do with these Nmap scripts?

The **Nmap Scripting Engine (NSE)** is incredibly versatile, and its scripts empower users to perform a wide range of tasks beyond basic port scanning. Here's what you can do with these scripts:

---

1. Vulnerability Detection

Identify vulnerabilities in systems and services:

- Check for **common exploits** (e.g., Heartbleed, SMBv1 vulnerabilities).
- Discover **misconfigurations** or **default credentials**.

Examples:

- Scan for vulnerabilities:

  ```
  nmap --script vuln <target>
  ```

- Specific vulnerability checks:
  - **SSL Heartbleed**:

    ```
    nmap --script ssl-heartbleed <target>
    ```

  - **SMB vulnerabilities**:

    ```
    nmap --script smb-vuln-* <target>
    ```

---

2. Brute-Forcing Authentication

Test logins for various services with brute-force attacks:

- FTP, SSH, HTTP forms, etc.

Examples:

- Brute-force FTP login:

  ```
  nmap --script ftp-brute <target>
  ```

- Brute-force HTTP forms:

  ```
  nmap --script http-form-brute --script-args
  userdb=/path/to/users.txt,passdb=/path/to/passwords.txt <target>
  ```

---

3. Service and Version Detection

Gather detailed information about services running on open ports:

- Identify software versions.
- Detect service configurations.

Examples:

- Find HTTP service titles:

```
nmap --script http-title <target>
```

- Check SSL certificate details:

```
nmap --script ssl-cert <target>
```

---

4. Information Gathering

Retrieve valuable reconnaissance data:

- DNS records.
- HTTP server headers.
- Network shares.

Examples:

- Enumerate DNS records:

```
nmap --script dns-brute <target>
```

- Fetch HTTP headers:

```
nmap --script http-headers <target>
```

---

5. Malware and Exploit Detection

Detect signs of malware or exploit activity:

- Identify backdoors or compromised services.

Examples:

- Detect Conficker worm:

```
nmap --script smb-check-vulns --script-args=unsafe=1 <target>
```

- Scan for malware-infected hosts:

```
nmap --script malware-host <target>
```

---

6. Network Discovery

Explore and map networks:

- Find live hosts.
- Discover shared resources.

Examples:

- Discover network shares via SMB:

```
nmap --script smb-enum-shares <target>
```

- Identify devices on the network:

```
nmap --script broadcast-ping <target>
```

---

7. Exploitation

Execute scripts that actively exploit vulnerabilities:

- These are often intrusive and may disrupt services.

Examples:

- Exploit FTP bounce vulnerability:

```
nmap --script ftp-bounce <target>
```

- Exploit HTTP vulnerabilities:

```
nmap --script http-slowloris <target>
```

---

8. Firewall and IDS/IPS Testing

Test the behavior and configuration of firewalls or intrusion detection/prevention systems.

Examples:

- Detect firewall rules:

```
nmap --script firewall-bypass <target>
```

- Test IDS/IPS evasion:

```
nmap -sS --script intrusive <target>
```

---

9. Password Auditing

Test for weak or default passwords:

- Check various protocols like SMB, MySQL, or RDP.

Examples:

- SMB password auditing:

```
nmap --script smb-brute <target>
```

- MySQL password brute-forcing:

```
nmap --script mysql-brute <target>
```

---

10. Custom Tasks

Write your own NSE scripts for specialized tasks:

- Automate repetitive scanning processes.
- Test for organization-specific vulnerabilities.

Example:

Create a Lua script to query a proprietary API and scan services.

Benefits of Using NSE Scripts

- **Automation**: Saves time by automating repetitive scanning tasks.
- **Versatility**: From discovery to exploitation, scripts cover diverse needs.
- **Extensibility**: Lua scripting allows for the creation of custom scripts.
- **Powerful Results**: Combine scripts with other Nmap options for highly customized scans.